Exhibit 4

United States District Court

EASTERN DISTRICT OF NEW YORK

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

THE PREMISES KNOWN AND DESCRIBED AS 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK (THE "SUBJECT PREMISES")

SEARCH WARRANT

CASE NUMBER:

13 M 0239

TO: Special Agent Aaron Spivack and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Aaron Spivack (Affiant) who has reason to

believe that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

THE PREMISES KNOWN AND DESCRIBED AS 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK (THE "SUBJECT PREMISES") as further described in Attachment A

in the EASTERN District of NEW YORK there is now concealed a certain person or property, namely (describe the person or property)

The items described in Attachment B.

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before April 2, 2013 (Date)

(not to exceed 14 days) the person or place named above for the person or property specified, serving this warrant and making the search (~~in the daytime - 6:00 A.M. to 10:00 P.M.~~)(at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Duty Magistrate (United States Judge or Magistrate Judge) as required by law.

March 19, 2013 at 11:25 AM (Date and Time Issued) at Brooklyn, New York (City and State)

Hon. Roanne L. Mann, U.S.M.J. (Name and Title of Judicial Officer)

Roanne L. Mann (Signature of Judicial Officer)

ATTACHMENT A

Property to be Searched

The SUBJECT PREMISES is located at 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK. The SUBJECT PREMISES is located in a red-brick building, which is approximately three stories tall. There are three white doors on the front of the building. The door to the SUBJECT PREMISES is down a set of stairs on the right side of the front of the building. There are two other doors at the top of a short set of steps. One of those doors has the numbers 1153 immediately above it.

ATTACHMENT B

Particular Things to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2251, 2252 and 2252A, and Title 21, United States Code, Section 844:

1. Dramamine, Benadryl, Valium, or other prescription or non-prescription drugs or medicines or substances that could be used to alter consciousness or incapacitate a child

2. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the production, possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, in any form wherever they may be stored or found;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of

minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

b. ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer related equipment, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be parents or guardians of minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be parents or guardians of minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Narcotics and narcotics paraphernalia, including but not limited to, scales, cutting agents, wrapping materials (including plastic bags and rubber bands), discarded wrappers and other materials used to conceal and transport narcotics, and machines used to package narcotics, such as heat-sealing machines.

16. All documents, text messages, "chat," or instant messages, call logs, and any other electronically-stored data (whether on cellular telephones or elsewhere) relating to conspiracy to produce child pornography or attempts to produce child pornography.

17. Cameras, and any other devices capable of taking photographs whether digital or otherwise, including camera-enabled cellphones and tablet computers.

18. Any computers, computer hard drives, or other physical objects upon which computer data can be recorded, including tablet computers, cellular telephones capable of acting as computers and media servers (including iPads, iPhones and AppleTVs) (hereinafter, "COMPUTER") that were or may have been used as a means to commit violations of 18 United States Code, Sections 2252 and 2252A. All information obtained from such computers or electronic media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the

purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:

a. any evidence described in this Attachment;

b. evidence of who used, owned, or controlled any computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography. Such information tends to show the identity of the person using the computer near the time of the criminal activity;

c. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

g. evidence of the times the computer was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the computer;

i. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

j. evidence of Peer to Peer software;

k. contextual information necessary to understand the evidence described in this attachment.

If any materials protected by the Privacy Protection Act, 42 U.S.C. § 2000aa are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

19. Records and things evidencing the use of any IP address, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

20. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A and Title 21, United States Code, Section 844.

Definitions

a. "Child Erotica," as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually

explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices

(including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "IP Address" as used herein, the IP Address or Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses,

while other computers have dynamic—that is, frequently changed—IP addresses.

j. "Wireless telephone": A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

k. "Digital camera": A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

l. "Portable media player": A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also

store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

p. "GPS": A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

q. "PDA": A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same

capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Tablet": A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

s. "Pager": A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

t. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

13 M 0239

JDL:TJS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- against -

THE PREMISES KNOWN AND DESCRIBED AS 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK
(THE "SUBJECT PREMISES")

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

(T. 18, U.S.C., §§ 2251, 2252 and 2252A; T. 21 U.S.C., § 844)

EASTERN DISTRICT OF NEW YORK, SS:

AARON SPIVACK, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such:

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK (hereinafter referred to as the "SUBJECT PREMISES"), the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution, reproduction attempted production and conspiracy to produce sexually explicit material relating to children, in

violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, and possession of narcotics, in violation of Title 21, United States Code, Section 844.

The source of my information and the grounds for my belief are as follows:[1]

AGENT BACKGROUND

1. I have been employed as a Special Agent with the FBI since 2008 and am currently assigned to the New York Office. For approximately three years, I have been assigned to a Crimes Against Children squad. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. I have participated in a number of investigations into the receipt, possession, and/or distribution of child pornography by electronic means, as well as the sexual enticement of minors. As part of my responsibilities, I have been involved in the investigation of numerous child pornography

---

[1] Because the purpose of this Affidavit is to set forth only those facts necessary to establish probable cause to search, I have not set forth all of the facts and circumstances of which I am aware.

cases and have reviewed hundreds of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I have also gained expertise regarding the use of computers in connection with crimes against children. I have received training relating to the use of computers by offenders and gained expertise through participating in numerous cases in which computers were used to facilitate crimes against children.

2. I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

INTRODUCTION

3. This affidavit is in support of an application to search the SUBJECT PREMISES. For the reasons set forth below, I

believe there is probable cause to believe that computerized and other information is contained within the SUBJECT PREMISES that is evidence or fruits or instrumentalities of offenses relating to the possession, access with intent to view, transportation, receipt, distribution, reproduction attempted production and conspiracy to produce sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, and possession of narcotics, in violation of Title 21, United States Code, Section 844. The items to be searched for and seized are specifically described in Attachment B to this affidavit which is incorporated herein.

THE SUBJECT PREMISES

4. The SUBJECT PREMISES is located at 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK. The SUBJECT PREMISES is located in a red-brick building, which is approximately three stories tall. There are three white doors on the front of the building. The door to the SUBJECT PREMISES is down a set of stairs on the right side of the front of the building. There are two other doors at the top of a short set of steps. One of those doors has the numbers 1153 immediately above it.

PROBABLE CAUSE

5. On or about February 13, 2013, a Confidential Source ("CS 1") reported to the FBI that an associate of CS 1, BEBARS BASLAN and BASLAN's girlfriend KRISTEN HENRY, possess child pornography and are preparing to sexually exploit children. CS 1 indicated that BASLAN told CS 1 that BASLAN and HENRY plan on opening a babysitting business as a cover to drug and sexually abuse children. CS 1 further stated that in order to protect himself BASLAN wants collateral he can use to blackmail HENRY, so BASLAN has asked CS 1 to provide his one-and-a-half-year-old son ("VICTIM 1") to BASLAN so HENRY can be photographed giving oral sex to VICTIM 1. CS 1 also indicated that BASLAN indicated he obtained child pornography from Internet newsgroups. Prior to February 13, 2013, CS 1 was not a Confidential Source of the FBI. The information provided by CS 1 has been corroborated by subsequent recordings as discussed below. CS 1 may face criminal charges in the future and is cooperating, in part, with the hope of reducing his ultimate sentence.

6. Following this meeting, CS 1 made numerous consensually recorded telephone calls with BASLAN at the

direction of the FBI. CS 1 recorded the following conversations, among others, excerpted portions of which are provided in sum and substance and in part below:

a. On February 24, 2013 at approximately 6:30 p.m., CS 1 had a recorded conversation with BASLAN over the telephone regarding BASLAN's plans to take pictures of HENRY engaging in sexual contact with VICTIM 1. During the conversation, BASLAN stated that he wanted HENRY to take a picture "as if you [CS 1] dropped him off to babysit, she [HENRY] took a picture and he [BASLAN] found it." CS 1 asked what HENRY would be doing with VICTIM 1. BASLAN indicated "blow." BASLAN stated it would be "hot watching her." BASLAN stated that he wants HENRY to "make a little video of her blowing whatever, him wouldn't even know what's going on." BASLAN then stated that he wanted to have "some safety" on HENRY because of her involvement in the plan to babysit children and drug and abuse them, and that "I just want to make sure I secure her". CS 1 stated that VICTIM 1 is one and a half years old and thathe wanted to ensure that whatever BASLAN wanted HENRY to do would not affect VICTIM 1 mentally.

BASLAN stated that HENRY would "be pretending to diaper change him and just take a couple pictures with her sucking him off". After some additional conversation, the call appeared to be disconnected unexpectedly.

b. On February 24, 2013 at approximately 6:40 pm, BASLAN and CS 1 had another telephone conversation, which CS 1 recorded. During the conversation, BASLAN stated that HENRY is "dying for this," referring to the plan to have HENRY sexually abuse VICTIM 1. CS 1 expressed concerns of the "mental stability" of VICTIM 1, and BASLAN stated "if it's one minute he won't even know what's going on," and "I think what we can do is also cover up his face really quick, as if you like pretend your tickling him or something, and she just takes the pose, she doesn't actually do anything, she just takes the pose. You understand what I mean?" BASLAN stated "I'm not looking for an actual thing to happen. I'm just looking for the pose of it. You could for all I care be on the other side, like, covering his face or whatever, and she just can do two licks or whatever and he wouldn't know the difference between

her cleaning him or her doing whatever". The call was then ended by CS 1.

c. On February 24, 2013 at approximately 6:55 pm, BASLAN and CS 1 had another telephone conversation, which CS 1 recorded. They had a discussion of what HENRY would do with VICTIM 1. BASLAN indicated that HENRY did not need to perform the act and that it just needs to look like it is being performed. Shortly after this, BASLAN and CS 1 had the following exchange:

BASLAN: I'm not looking for it to be anything physical and the other stuff is all going to be when the person is passed out, so it's not going to be like anything that happened to us.[2]

CS 1: Like for babysitting gig, you're going to do the roofies, so it won't affect them…

BASLAN: Exactly, they're going to be. . .no memories, nothing. It's just you know. . .

CS 1: There's no harm being done.

BASLAN: Right exactly, they're going to be asleep.

Later during the conversation, BASLAN stated that HENRY is "dying for me to have a baby with her for us

---

[2] CS 1 understood the phrase "it's not going to be like anything that happened to us" is a reference to sexual abuse that BASLAN and CS 1 both suffered as children.

to whatever." CS 1 then asked "The two of you having your own kid and then you raise it in a sexual upbringing kind of thing?" BASLAN responded, "Right." Later during the conversation, BASLAN and CS 1 discussed CS 1's niece, who is six years old, (VICTIM 2). BASLAN indicated that HENRY really wanted to babysit VICTIM 2, which CS 1 understood to mean that HENRY wanted to sexually abuse VICTIM 2. BASLAN stated maybe they could arrange something in the next few weeks. BASLAN stated that HENRY wanted to use "kids Dramamine" to drug the children and that they could "rub it in their mouth a little bit".

7. On March 7, 2013, CS 1, who was equipped with electronic monitoring devices including audio recorders and a video recorder, met with BASLAN and HENRY at the SUBJECT PREMISES. During the meeting, CS 1 recorded BASLAN and HENRY discussing their plan to meet at a hotel in New Jersey to take sexually explicit photographs of HENRY and VICTIM 1. HENRY was present during those conversations. During the meeting, CS 1 told BASLAN that he did not want VICTIM 1 to "wake up or know anything at all" and asked BASLAN what would be the best thing to give VICTIM 1. BASLAN asked how old VICTIM 1 was and CS 1

stated a year and a half. BASLAN stated "for sure Dramamine". BASLAN told CS 1 that he had Valium that he could "split into a tenth of a milligram", and that he looked up the dosages based on height and weight and that you could give a child the "powder, a puff".

8. During the March 7, 2013 meeting, BASLAN also told CS 1 that he would bring his laptop to the hotel and watch "some videos." CS 1 understood BASLAN to mean videos of child pornography. BASLAN described a video he has in which a man has sex with his wife, his wife's sister, and a little girl who BASLAN describes as five or six years old.

9. Later during the meeting, BASLAN used his computer to access child pornography which was played on BASLAN's television while BASLAN, HENRY, and CS 1 were present. Some of the child pornography videos were captured on CS 1's video recording device. The videos appeared to depict prepubescent girls being vaginally and orally penetrated by an adult man's penises. Some of the videos had sound, and the children can be heard. HENRY commented regarding one of the child pornography videos that it was the "hottest one." BASLAN described to CS 1 that the child pornography in his residence can be accessed on his Ipad,

Iphone, and television, and that the devices were accessing the child pornography from a central location. BASLAN told CS 1 that he uses encryption that he created, and that his files are "unhackable". BASLAN indicated that he deletes his child pornography.

10. During the meeting, BASLAN told CS 1 that he has a babysitting job lined up but that they have to do the take the sexually explicit picture with VICTIM 1 first. BASLAN stated that the child they have lined up to babysit is between the ages of four and six years old ("VICTIM 3"). HENRY stated that she had worked in the school system for several years, has "excellent references," and that as a teenager she used to babysit and could get references that way. BASLAN stated that once they had someone to babysit they could slip something in the child's drink. CS 1 asked HENRY if she had ever done this before, and HENRY stated that she had not. HENRY told CS 1 that when she was young she would have "sub-conscious scenarios" and that BASLAN was the first person she ever confided her interests in.

11. During the meeting, BASLAN, HENRY, and CS 1 also discussed narcotics. HENRY mentioned that "mushrooms" were

likely present in the SUBJECT PREMISES, and BASLAN discussed purchasing cocaine from someone that night. BASLAN asked CS 1 how much he wanted and CS 1 stated "one bag or two bags". BASLAN stated he was getting two bags for himself. As short time later, BASLAN made a call on his telephone and stated that he "need[ed] four tickets."

12. Before CS 1 left the SUBJECT PREMISES on March 7, 2013, BASLAN asked CS 1 about CS 1's eight-year-old daughter (VICTIM 4), and asked if HENRY could "go down" on her. CS 1 then left the SUBJECT PREMISES but stated that he would return with the money for the narcotics.

13. Later on March 07, 2013, CS 1 called BASLAN to discuss CS 1 paying BASLAN for narcotics. CS 1 asked BASLAN if BASLAN could leave the SUBJECT PREMISES to retrieve money for the narcotics. BASLAN agreed and CS 1 retrieved $100.00 and returned to the SUBJECT PREMISES where BASLAN met him outside. CS 1 gave BASLAN the $100.00 and BASLAN went to another vehicle and retrieved the narcotics. BASLAN then went back to CS 1 and provided him with two bags of a white substance, and BASLAN kept two bags for himself. CS 1 left the area then and met with law

enforcement agents. CS 1 provided law enforcement agents with approximately .8 grams of cocaine.

14. Shortly after that, CS 1 called BASLAN to discuss the cocaine CS 1 had just purchased. CS 1 stated that he thought the bags looked "light". BASLAN stated that his were fine and that he weighed the bags and they were "point seven, point eight" and that there is "not a refund policy".

15. A search through US Postal Service databases indicates that BASLAN and HENRY moved into the SUBJECT PREMISES in January, 2013, and occupy the basement and apartment 1.

16. I have been informed by an Assistant U.S. Attorney that the Second Circuit has noted, "[w]hen a defendant is suspected of possessing child pornography, the staleness determination is unique because it is well known that 'images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes.'" United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006)(quoting United States v. Lamb, 945 F. Supp. 441, 459-60 (N.D.N.Y. 1996)). In Irving, the Second Circuit upheld a search based upon information which was more than 22 months old, noting that even though the affidavit disclosed that the defendant took care

to destroy inappropriate photographs, that "there was a fair probability that child pornography would be found. . ." Id. Thus, under the relevant case law, information in support of probable cause in child pornography cases is often not deemed stale, even if somewhat old, because collectors and traders of child pornography are known to store and retain their collections for extended periods of time, usually in their home and/or on their computer. See e.g., United States v. Seiver, ___ F.3d ___, 2012 WL 3686387, (7th Cir. August 28, 2012)("'Staleness' is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file. Computers and computer equipment are not the type of evidence that rapidly dissipates or degrades." As such, "[o]nly in the exceptional case should a warrant to search a computer for child pornography be denied on [staleness grounds].") (citations and internal quotations omitted); United States v. Allen, 625 F.3d 830 (5th Cir. 2010)(18-month delay between time period that child pornography images were accessed by defendant from peer-to-peer networking site and issuance of search warrant did not render the information stale); United States v. Pappas, 592 F.3d 799 (7th Cir. 2010)(officers reasonably could have relied on the

search warrant that was based on child pornography sent eighteen months earlier); United States v. Ricciardelli, 998 F.2d 8, 12, n. 4 (1st Cir. 1993) (stating that "history teaches that collectors [of child pornography] prefer not to dispose of their dross, typically retaining obscene materials for years"); United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000) (concluding six month old information supporting probable cause was not stale because (a) collectors of child pornography are likely to retain their sexually explicit materials; and (b) even if deleted, it is possible that the sexually explicit images could be recovered by a computer expert); United States v. Chroback, 289 F.3d 1043, 1046 (8th Cir. 2002) (finding three month old information sufficient to establish probable cause, when viewed in the totality of the circumstances, because collectors of child pornography tend to maintain their materials in a secure place for extended periods); United States v. Roby, 27 Fed. Appx. 779, 780 (9th Cir. 2001) (unpub.) (eight and one half months since the time defendant downloaded child pornography did not render the information relied on in the warrant stale); United States v. Anderson, 187 F.3d 649, 1999 WL 459586, at *1-2 (9th Cir. July 6, 1999) (table) (eleven month old information established probable cause where supported by expert opinion that

established that child pornography collectors and pedophiles retain their contraband for long periods of time); United States v. Sassani, 139 F.3d 895, 1998 WL 89875, at *4 (4th Cir. Mar. 4, 1998) (table) (six month old information); United States v. Lacy, 119 F.3d 742, 745-46 (9th Cir. 1997) (ten month old information in support of probable cause was not stale; affidavit stated that collectors of child pornography "rarely if ever" dispose of child pornography, and store it "for long periods" of time in a secure place, typically in their homes); United States v. Lamb, 945 F. Supp. 441, 459-60 (N.D.N.Y. 1996) (holding warrant information not stale despite five month lapse since last transmission of child pornography over Internet); United States v. Bateman, 805 F. Supp. 1041, 1044 (D.N.H. 1992) (upholding warrant with seven month delay between distribution of child pornography and execution of warrant); United States v. Rakowski, 714 F. Supp. 1324, 1330 (D. Vt. 1987) (upholding warrant based on information one to six months old because "those who collect child pornography keep the pornography, do not destroy their collections, and keep the pornography accessible"); United States v. Horn, 187 F.3d 781, 786-87 (8th Cir. 1999) ("lapse of time is least important when the suspected criminal activity is continuing in nature and when the property

is not likely to be destroyed or dissipated" and probable cause was not stale where the defendant had demonstrated a "deep and continuing interest in his [child pornography] collection" and it was likely that he would retain child pornography for that collection); United States v. Albert, 195 F. Supp. 2d 267, 277 (D. Mass. 2002) (concluding that, despite a four month lapse, affidavit supported a finding of probable cause where the defendant maintained a deep and continuing interest in his collection of child pornography); United States v. Shields, 2004 WL 832937, *8 (M.D.Pa. 2004) (holding that a staleness claim was devoid of merit, where the nine month period was at issue, as "collectors of child pornography frequently possess and retain pornographic images over extended periods"); United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (more than three years); United States v. Gourde, 440 F.3d 1065, 1071 (9th Cir. 2006)("Having paid for multi-month access to a child pornography site, Gourde was also stuck with the near certainty that his computer would contain evidence of a crime had he received or downloaded images in violation of § 2252. Thanks to the long memory of computers, any evidence of a crime was almost certainly still on his computer, even if he had tried to delete the images. FBI computer experts, cited in the affidavit,

stated that 'even if ... graphic image files [ ] have been deleted ... these files can easily be restored.' In other words, his computer would contain at least the digital footprint of the images.") (eight months from subscription to execution of search warrant); United States v. Toups, 2007 WL 433562 (M.D. Ala. February 6, 2007) ("Further bolstering the conclusion that the staleness calculation is unique when it comes to cases of Internet child pornography is the images and videos stored on a computer are not easily eliminated from a computer's hard drive. The mere deletion of a particular file does not necessarily mean that the file cannot later be retrieved).

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and

directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

DEFINITIONS

18. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

a. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital,

oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]" It includes cellular telephones

e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard

drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as modems, routers, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming

code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice

communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

i. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the

stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

j. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

k. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location.

These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

1. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable

storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

m. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing

the Web, sending and receiving e-mail, and participating in Internet social networks.

n. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital

Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, drives, or electronic notebooks and tablets, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose

of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to

draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to receive or distribute child pornography, the individual's computer will generally serve both as an

instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

22. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the

accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

23. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not

limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

24. Based on my training and experience, I am aware that the sheer size of child pornography Internet files makes it difficult for the child pornography viewer/collector to maintain these files solely on his/her computer. Thus, when executing search warrants in child pornography cases, agents have often found CDs, DVDS, thumb drives, and other alternate forms of portable storage devices on which the child pornography viewer/collector has stored the pornography.[3] In addition,

---

[3] I understand from experienced investigators that individuals who collect child pornography typically have multiple computers and other devices capable of accessing or storing child pornography (in fact, most residences now have multiple devices capable of accessing the internet and storing images). There is no way to determine prior to forensic examination, which device accessed a given IP address under investigation or whether child pornography has been moved from that device into another device. As such, it is necessary to search any device capable of accessing or storing child pornography. Given the state of current technology, virtually any object may be such a repository for child pornography. For instance, digital watches, mobile phones, MP3 players, video game systems and digital cameras are all examples of devices which may be used to store digital images of child pornography. Moreover, such

agents have often found handwritten notations in notebooks, etc., where the child pornography viewer/collector has written various IP addresses of child pornography internet sites, so that he/she may easily visit the site again. It is also my experience that individuals who collect and trade video images of child pornography also use written notes or printouts related to their Internet activity concerning child pornography, including, but not limited to passwords, lists of websites, filenames or lists of child pornography series.

25. Based on the nature of this case, it may become necessary to arrest BASLAN and HENRY quickly if they have access to children whom they may then molest. This may happen at any hour of the day or night. Based on my training and experience, I am aware that it is possible to remotely trigger the destruction of computer files. Based on BASLAN's computer expertise, I believe it will be necessary to conduct a search of the SUBJECT PREMISES shortly after his arrest to secure evidence before he could potentially by himself or using a third party trigger the destruction of computer files remotely. For that

---

devices meet the definition of a "computer" pursuant to Title 18, United States Code, Section 1030(e)(1).

reason, I request that the Court authorize that this search warrant may be carried out at any time of the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Aaron Spivack
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on March 19, 2013:

THE HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The SUBJECT PREMISES is located at 1153 OCEAN PARKWAY, BASEMENT, BROOKLYN, NEW YORK. The SUBJECT PREMISES is located in a red-brick building, which is approximately three stories tall. There are three white doors on the front of the building. The door to the SUBJECT PREMISES is down a set of stairs on the right side of the front of the building. There are two other doors at the top of a short set of steps. One of those doors has the numbers 1153 immediately above it.

ATTACHMENT B

Particular Things to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2251, 2252 and 2252A, and Title 21, United States Code, Section 844:

1. Dramamine, Benadryl, Valium, or other prescription or non-prescription drugs or medicines or substances that could be used to alter consciousness or incapacitate a child

2. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the production, possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, in any form wherever they may be stored or found;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of

minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

b. ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer related equipment, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be parents or guardians of minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be parents or guardians of minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Narcotics and narcotics paraphernalia, including but not limited to, scales, cutting agents, wrapping materials (including plastic bags and rubber bands), discarded wrappers and other materials used to conceal and transport narcotics, and machines used to package narcotics, such as heat-sealing machines.

16. All documents, text messages, "chat," or instant messages, call logs, and any other electronically-stored data (whether on cellular telephones or elsewhere) relating to conspiracy to produce child pornography or attempts to produce child pornography.

17. Cameras, and any other devices capable of taking photographs whether digital or otherwise, including camera-enabled cellphones and tablet computers.

18. Any computers, computer hard drives, or other physical objects upon which computer data can be recorded, including tablet computers, cellular telephones capable of acting as computers and media servers (including iPads, iPhones and AppleTVs) (hereinafter, "COMPUTER") that were or may have been used as a means to commit violations of 18 United States Code, Sections 2252 and 2252A. All information obtained from such computers or electronic media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the

purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:

a. any evidence described in this Attachment;

b. evidence of who used, owned, or controlled any computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography. Such information tends to show the identity of the person using the computer near the time of the criminal activity;

c. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

g. evidence of the times the computer was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the computer;

i. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

j. evidence of Peer to Peer software;

k. contextual information necessary to understand the evidence described in this attachment.

If any materials protected by the Privacy Protection Act, 42 U.S.C. § 2000aa are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

19. Records and things evidencing the use of any IP address, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

20. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A and Title 21, United States Code, Section 844.

Definitions

a. "Child Erotica," as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually

explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices

(including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "IP Address" as used herein, the IP Address or Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses,

while other computers have dynamic—that is, frequently changed—IP addresses.

j. "Wireless telephone": A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

k. "Digital camera": A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

l. "Portable media player": A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also

store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

p. "GPS": A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

q. "PDA": A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same

capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Tablet": A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

s. "Pager": A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

t. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).